WHAT IS CLAIMED

1.A method for obtaining a shared secret key, comprising the steps of:

identifying a first shared random number;

identifying a second shared random number; and

obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

2. The method of claim 1, wherein said combining function includes a logical function.

3. The method of claim 2, wherein said logical function includes an exclusive or (XOR) function.

4. A method for obtaining a shared secret key utilized in a network having at least a first computer and a second computer, said method comprising the steps of:

transmitting a first message from said first computer to said second computer, said first message including a first shared random number;

generating a second shared random number in said second computer; and

generating a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

5. The method of claim 4, further comprising the step of transmitting a second message from said second computer to said first computer, said second message including said second shared random number.

6. The method of claim 5, wherein said first message is encoded using an encoded password.

7. The method of claim 6, wherein said encoded password is an encrypted password.

8. The method of claim 6, wherein said step of encoding said first message comprises encrypting said first message using said encoded password.

9. The method of claim 5, wherein said first message also includes an asymmetric key.

10. The method of claim 9, wherein said second message is encoded using said asymmetric key.

11. The method of claim 10, wherein said second message is encrypted using said asymmetric key.

12. The method of claim 5, wherein said combining function includes a logical function.

13. The method of claim 12, wherein said logical function includes an exclusive or (XOR) function.

14 ~~13~~. An electronic data signal including information encoded using a shared secret key, wherein said shared secret key is obtained from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

15 ~~14~~. The data signal of claim 13, wherein said data signal is propagated through a network.

16 ~~15~~. The data signal of claim 13, wherein said information is encoded using said shared secret key.

17 ~~16~~. The data signal of claim 15, wherein said information is encrypted using said shared secret key.

18 ~~17~~. The signal of claim 13, wherein said signal comprises a packet of data representing a portion of said information.

19 ~~18~~. The signal of claim 13, wherein said signal is a wireless signal.

20 ~~19~~. The signal of claim 13, wherein said signal is embedded in a carrier wave.

21 ~~20~~. The signal of claim 13, wherein said signal is propagated as an analog signal.

22 ~~21~~. The signal of claim 13, wherein said signal is propagated as a digital signal.

23 ~~22~~. The signal of claim 13, wherein said combining function includes a logical function.

24 ~~23~~. The method of claim 22, wherein said logical function includes an exclusive or (XOR) function.

25 ~~24~~. A method for obtaining a shared secret key, comprising the steps of:

receiving a first message including a first shared random number;

identifying a second shared random number;

obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

26 ~~25~~. The method of claim 24, further comprising the step of transmitting a second message including said second shared random number.

27 ~~26~~. The method of claim 25, wherein said step of identifying a second shared random number comprises generating said second shared random number.

28 ~~27~~. The method of claim 25, wherein said first message is encoded using a first key obtained using information obtained from a password.

29 ~~28~~. The method of claim 27, wherein said first message is encoded using a first key obtained using information obtained from a password.

30 ~~29~~. The method of claim 28, wherein said first message is encrypted using a first key obtained using information obtained from a password.

31 ~~30~~. The method of claim 27, wherein said first key is obtained by encoding said password.

32 ~~31~~. The method of claim 30, wherein said step of encoding said password comprises encrypting said password.

33 ~~32~~. The method of claim 27, wherein said first message also includes a second key.

34 ~~33~~. The method of claim 32, wherein said second key is an asymmetric key.

35 ~~34~~. The method of claim 32, wherein said second message is encoded with said second key.

36 ~~35~~. The method of claim 34, wherein said second message is encrypted with said second key.

37 ~~36~~. The method of claim 32, further comprising receiving said password from a user.

38 ~~37~~. The method of claim 24, wherein said combining function includes a logical function.

39 ~~38~~. The method of claim 24, wherein said logical function includes an exclusive or (XOR) function.

40 ~~39~~. The method of claim 27, wherein said first key is generated using an encoded password obtained from said password.

41 ~~40~~. The method of claim 39, wherein said encoded password is an encrypted password.

42 ~~41~~. The method of claim 40, wherein said encrypted password is obtained from an output of a one-way function having an input including said password.

43 ~~42~~. The method of claim 41, wherein said one-way function is a hash function.

44 ~~43~~. The method of claim 27, further comprising the step of receiving said password from a user.

45 ~~44~~. The method of claim 43, further comprising transmitting information identifying said user.

46 ~~45~~ The method of claim 43, wherein said user is a human user.

47 ~~46~~. The method of claim 43, further comprising the step of obtaining said first key from an output of a one-way function having an input including said password.

48 ~~47.~~ The method of claim 43, further comprising decrypting said first message using information obtained from said password.

49 ~~48.~~ The method of claim 27, further comprising transmitting identification information for a user.

50 ~~49.~~ The method of claim 27, wherein said first message also includes a second key.

51 ~~50.~~ The method of claim 49, wherein said second key is an asymmetric key.

52 ~~51.~~ The method of claim 50, wherein said second message is encoded with said second key.

53 ~~52.~~ The method of claim 37, wherein said second message is encrypted with said second key.

54 ~~38.~~ The method of claim 51, wherein said second message also includes a timestamp.

55 ~~54.~~ The method of claim 27, wherein said first message also includes a timestamp.

56 ~~55.~~ The method of claim 27, wherein said first message also includes a second key and a timestamp.

57 ~~56.~~ The method of claim 55, wherein said second key is an asymmetric key.

58 ~~57.~~ A device including at least one processor, said at least one processor executing software instructions for obtaining a shared secret key, said software instructions comprising a software module identifying a first shared random number and a second shared random number and obtaining the shared secret keybased on said first shared random number and said second shared random number, wherein the device is capable of transforming messages using the shared secret key.

59 ~~58.~~ The device of claim 57, wherein the first shared random number is communicated to a user.

60 ~~59.~~ The device of claim 58, wherein the shared secret key is obtained from said user.

61 ~~60.~~ The device of claim 57, wherein the shared secret key is obtained from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

62 ~~61.~~ The method of claim 60, wherein said step of identifying a first shared random number comprises generating said first shared random number.

63 ~~62.~~ The method of claim 61, wherein said step of identifying a second shared random number comprises receiving a second message including said second shared random number.

64 ~~63.~~ The method of claim 60, wherein said step of identifying a second shared random number comprises generating said second shared random number.

65 ~~64.~~ The method of claim 63, wherein said step of identifying a first shared random number comprises receiving a first message including said first shared random number.

66 ~~65~~. The device of claim 60, wherein said device is capable of transforming messages by encoding messages using the shared secret key.

67 ~~66~~. The device of claim 65, wherein said encoding messages using the shared secret key comprises encrypting messages using the shared secret key.

68 ~~67~~. The device of claim 60, wherein said device is capable of transforming messages by decoding messages using the shared secret key.

69 ~~68~~. The device of claim 67, wherein said decoding messages using the shared secret key comprises decrypting messages using the shared secret key.

70 ~~69~~. The device of claim 60, wherein said device comprises a computer.

71 ~~70~~. The device of claim 60, wherein said device comprises a handheld device.

72 ~~71~~. The device of claim 60, further comprising a memory coupled to said processor, wherein at least a portion of said software module is stored in said memory.

73 ~~72~~. A device including at least one processor, said at least one processor executing software instructions for obtaining a shared secret key, said software instructions comprising a software module parsing a first message including a first shared random number to identify said first shared random number, identifying a second shared random number, and obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number, wherein the shared secret key is used by the device to transform messages.

74 ~~73~~. The device of claim 72, wherein said device decrypts said first message.

75 ~~74~~. The method of claim 72, wherein said step of identifying a second shared random number comprises generating said second shared random number.

76 ~~75~~. The device of claim 72, wherein said device transmits a second message including the second shared random number.

77 ~~76~~. The device of claim 75, wherein said first message is encoded using a first key obtained using information obtained from a password.

78 ~~77~~. The device of claim 76, wherein said first message is encrypted using a first key obtained using information obtained from a password.

79 ~~78~~. The device of claim 76, wherein said first message also includes an asymmetric key.

80 ~~79~~. The device of claim 78, wherein said second message is encoded with said asymmetric key.

81 ~~80~~. The device of claim 79, wherein said second message is encrypted with said asymmetric key.

82 ~~81~~. A device including at least one processor, said at least one processor executing software instructions for obtaining a shared secret key, said software instructions comprising a first software module identifying a first shared random number, parsing a second message including a second shared random number to identify said second shared random number, and obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number, wherein the shared secret key is used by the device to transform messages.

83 ~~82~~. The device of claim 81, wherein said device decrypts said second message.

84 ~~83~~. The method of claim 81, wherein said step of identifying a first shared random number comprises generating said first shared random number.

85 ~~84~~. The device of claim 81, wherein said software module generates a first message including said first shared random number.

86 ~~85~~. The device of claim 84, wherein said first message also includes a second key.

87 ~~86~~. The device of claim 85, wherein said first message also includes an asymmetric key.

88 ~~87~~. The device of claim 86, wherein said second message is encoded with said asymmetric key.

89 ~~88~~. The device of claim 87, wherein said second message is encrypted with said asymmetric key.

90 ~~89~~. The device of claim 85, wherein said first key corresponds to a password known by a user.

91 ~~90~~. A machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor, comprising:

encoded computer means for identifying a first shared random number;

encoded computer means for identifying a second shared random number; and

encoded computer means for obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

92 ~~91~~. A storage medium according to claim 90 wherein said storage medium is at least one of a group including semiconductor memory device, magnetic device, optical device, magneto-optical device, floppy diskette, hard drive, CD-ROM, magnetic tape, computer memory, and memory card.

93 ~~92~~. A storage medium according to claim 90, wherein said combining function includes a logical function.

94 ~~93~~. A storage medium according to claim 92 wherein said logical function includes an exclusive or (XOR) function.

95 ~~94~~. A machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor, comprising:

encoded computer means for parsing a first message including a first shared random number to obtain said first shared random number;

encoded computer means for identifying a second shared random number; and

encoded computer means for obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

96 ~~95~~. The storage medium of claim 94, further comprising encoded computer means for decrypting said first message.

97 ~~96~~. The storage medium of claim 94, further comprising encoded computer means for generating a second message including said second shared random number.

98 ~~97~~. The storage medium of claim 96, wherein said first message is encoded using a first key obtained using information obtained from a password.

99 ~~98~~. The storage medium of claim 97, wherein said first message is encrypted using a first key obtained using information obtained from a password.

100 ~~99~~. The storage medium of claim 97, wherein said first message also includes an asymmetric key.

101 ~~100~~. The storage medium of claim 99, wherein said second message is encoded with said asymmetric key.

102 ~~101~~. The storage medium of claim 100, wherein said second message is encrypted with said asymmetric key.

103 ~~102~~. A machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor, comprising:

encoded computer means for identifying a first shared random number;

encoded computer means for parsing a second message including a second shared random number to obtain said second shared random number; and

encoded computer means for obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

104 ~~103~~. The storage medium of claim 102, further comprising encoded computer means for decrypting said second message.

105 ~~104~~. The storage medium of claim 102, further comprising encoded computer means for transmitting a first message including said first shared random number.

106 ~~105~~. The storage medium of claim 104, wherein said first message also includes a second key.

107 ~~106~~. The storage medium of claim 105, wherein said second key is an asymmetric key.

108 ~~107~~. The storage medium of claim 106, wherein said second message is encoded with said asymmetric key.

109 ~~108~~. The storage medium of claim 107, wherein said second message is encrypted with said asymmetric key.

110 ~~109~~. The storage medium of claim 105, wherein said first message is encoded using a first key.

111 ~~110~~. The storage medium of claim 109, wherein said first message is encrypted using a first key.

112 ~~111~~. The storage medium of claim 109, wherein said first key corresponds to a password known by a user.

113 ~~112~~. A method for obtaining a shared secret key, comprising the steps of:

identifying a first shared random number;

receiving a second message including a second shared random number; and

obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

114 ~~113~~. The method of claim 112, further comprising the step of transmitting a first message including said first shared random number.

115 ~~114~~. The method of claim 113, wherein said step of identifying a first shared random number comprises generating said first shared random number.

116 ~~115~~. The method of claim 113, wherein said first message is encoded using a first key.

117 ~~116~~. The method of claim 115, wherein said first message is encrypted using a first key.

118 ~~117~~. The method of claim 115, wherein said first message also includes a second key.

119 ~~118~~. The method of claim 115, wherein said first key corresponds to a password.

120 ~~119~~. The method of claim 118, wherein said first key is an encoded password.

121 ~~120.~~ The method of claim 119, wherein said first key is an encrypted password.

122 ~~121.~~ The method of claim 118, wherein said step of obtaining the shared secret key comprises obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

123 ~~122.~~ The method of claim 121, wherein said combining function includes a logical function.

124 ~~123.~~ The method of claim 122, wherein said logical function includes an exclusive or (XOR) function.

125 ~~124.~~ The method of claim 117, wherein said second key is an asymmetric key.

126 ~~125.~~ The method of claim 117, wherein said second message is encoded with said second key.

127 ~~126.~~ The method of claim 125, wherein said second message is encrypted with said second key.

128 ~~127.~~ The method of claim 125, further comprising decoding said second message.

129 ~~128.~~ The method of claim 127, wherein said decoding said second message comprises decoding said second message using a third key.

130 ~~129.~~ The method of claim 128, wherein said third key and said second key form an asymmetric key pair.

131 ~~130.~~ The method of claim 129, further comprising the step of generating said asymmetric key pair.

132 ~~131.~~ The method of claim 130, wherein said asymmetric key pair is generated dynamically.

133 ~~132.~~ The method of claim 130, wherein said asymmetric key pair is selected from a set of pre-generated asymmetric key pairs.

134 ~~133.~~ The method of claim 115, further comprising receiving information identifying a user.

135 ~~134.~~ The method of claim 133, wherein said first key is associated with said user.

136 ~~135.~~ The method of claim 134, wherein said first key corresponds to a password known by said user.

137 ~~136.~~ The method of claim 135, wherein said first key is an encoded value of said password.

138 ~~137.~~ The method of claim 135, wherein said encoded value of said password is an encrypted value of said password.

139 ~~138.~~ The method of claim 136, wherein said first key is a value of said password after being sent through a one-way function.

140 ~~139~~. The method of claim 136, further comprising the step of obtaining said first key by looking up said user in a password file.

141 ~~140~~. The method of claim 139, wherein said password file contains an encoded password.

142 ~~141~~. The method of claim 140, wherein said encoded password is an encrypted password.

143 ~~142~~. The method of claim 139, wherein said password file is encoded.

144 ~~143~~. The method of claim 142, wherein said encoded password file is an encrypted password file.

145 ~~144~~. The method of claim 115, wherein said first message also includes a second key.

146 ~~145~~. The method of claim 144, wherein said second key is an asymmetric key.

147 ~~146~~. The method of claim 145, wherein said second message is encoded with said second key.

148 ~~147~~. The method of claim 146, wherein said second message is encrypted with said second key.

149 ~~148~~. The method of claim 146, wherein said second message also includes a timestamp.

150 ~~149~~. The method of claim 115, wherein said first message also includes a timestamp.

151 ~~150~~. The method of claim 115, wherein said first message also includes a second key and a timestamp.

152 ~~151~~. The method of claim 150, wherein said second key is an asymmetric key.